دراسة

إستراتيجية الكيان الصهيوني في إدارة الحرب الالكترونية



مقدمة:

تتناول هذه الدراسة التعريف بالحرب الالكترونية وعلاقتها بما يسمى "الفضاء الالكتروني"، إضافة إلى توضيح وجهة نظرة الكيان الصهيوني بالنسبة إلى هذا النوع من الحروب التي وصفها بعض المحللين بالحرب الإستراتيجية، وقد تم من خلال الدراسة استعراض أهم الدول المتنافسة حول العالم في هذا المجال مثل الولايات المتحدة، الصين، روسيا، انجلترا.

لقد انضم المجال الالكتروني على ما يبدو إلى جوار المجالات الأخرى (البرية، والبحرية، والجوية، والفضائية) للمشاركة في ميادين الحروب، حيث أنه من المتوقع أن تكون الحروب الالكترونية السمة الغالبة إن لم تكن الرئيسية للحروب المستقبلية في القرن ٢١.

تكمن خطورة حروب الانترنت وشبكات الاتصالات في كون العالم أصبح يعتمد بفاعلية أكثر مما مضى على الفضاء الالكتروني، لاسيما في مجال البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية، إضافة إلى المؤسسات والشركات العامة والخاصة.

تعريف لأهم مصطلحات الحرب الالكترونية

يقصد بالحرب الالكترونية على أنها أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الحواسيب والشبكات التابعة لدولة أخرى، بهدف تحقيق أضرار بالغة أو تعطيلها.

وعرفها آخرون بأنها مفهوم يشير إلى أي نزاع يحدث في الفضاء الالكتروني، ويكون له طابع دولي.

الفضاء الالكتروني:

هو عبارة عن مصطلح حديث ظهر في العقود الأخيرة، نتيجة لثورة تكنولوجيا المعلومات، ويشمل جميع الحواسيب والمعلومات التي بداخلها، والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الانترنت العامة.

أشكال النزاع في الفضاء الالكتروني:

تتعدد أشكال النزاع والصراع الالكتروني بين الدول في مختلف أنحاء العالم، ومن أشكال النزاع أو ما يسمى الحروب الالكترونية ما يلي:

١) القرصنة الالكترونية أو التخريب الالكتروني:

تحتل المرتبة الأولى من النزاع في الفضاء الالكتروني، وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء المحتوى، مثل ما يعرف بالملقمات (servers) من خلال إغراقها بالبيانات.

٢) الجريمة الالكترونية والتجسس الالكتروني:

تحتلان المرتبة الثانية والثالثة وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.

٣) الإرهاب الالكتروني:

يحتل المرتبة الرابعة من النزاع في الفضاء الالكتروني، وهو مصطلح يصف الهجمات غير الشرعية التي تنفذها مجموعات أو فاعلون غير حكوميون ضد أجهزة الحواسيب والشبكات والمعلومات المخزنة.

٤) الحرب الالكترونية:

وهي المستوى الأخطر للنزاع في الفضاء الالكتروني، وتعتبر جزءاً من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية وتوجهات المدنيين في مسرح العمليات الالكتروني.

حروب الانترنت:

هي حروب لا تناظرية ذات تكلفة متدنية نسبيا في أدواتها، وهذا يعني عدم الحاجة لتصنيع أسلحة مكلفة جداً وبالتالي فهي تتميز بعدة مميزات عالية وهي:

١. تمتع المهاجم بأفضلية واضحة في العمل من حيث السرعة والمرونة والمراوغة.
٢. استخدام سلاح يعتبر فتاكا من الناحية الإستراتيجية.

٣. إفشال لنماذج الردع المعروفة أمام هذه النوعية من الحروب.
٤. مخاطرها تتعدى استهداف المواقع العسكرية، باستهداف البنى التحتية المدنية والعسكرية الحساسة في البلدان المستهدفة.

الكيان الصهيوني وإستراتيجية الحرب الالكترونية

تتجه دولة الكيان الصهيوني نحو تفعيل سلاح الحرب الالكترونية " الهجمات الالكترونية " بجانب الأسلحة النارية التقليدية وغيرها، نظراً لفاعلية أدائها وآثارها المدمرة على اعتبار أن الحروب المستقبلية القادمة ستكون بأقل الضحايا ولكن خسائرها الإستراتيجية ستكون أكثر فداحة وحسمها العسكري أسرع.

التدابير التي اتخذها الكيان الصهيوني للدفاع عن الفضاء الالكتروني الصهيوني في مجال الحرب الالكترونية:

لقد اتخذ الكيان الصهيوني مجموعة من التدابير والخطوات في مجال الحرب الالكترونية في محاولة للدفاع عن الفضاء الالكتروني الصهيوني، فقام بإنشاء مجموعة من المؤسسات، والهيئات الخاصة بمجال الانترنت، لحماية البنية التحتية المدنية والعسكرية من أي هجوم معادي من قبل الأفراد أو المنظمات أو الدول.

١. البنية التحتية الحكومية لعصر الانترنت:

أقام الكيان الصهيوني في سنة ١٩٩٧م مشروع " بنية الحكومة التحتية لعصر الانترنت " في داخل وزارة المالية الصهيونية، وحدد هدف هذا المشروع حماية وتأمين استعمال الانترنت في الوزارات والمؤسسات الحكومية، وإيجاد حلول لمشاكل حماية المعلومات، وكذلك إجراء الأبحاث حول هذا الموضوع.

٢. السلطة الرسمية لحماية المعلومات:

أنشئت في سنة ٢٠٠٢م السلطة الرسمية لحماية المعلومات في داخل جهاز الأمن العام "الشاباك"، وكلفت هذه السلطة مهام حماية البنى التحتية للحواسيب الهامة والحيوية في الكيان من مخاطر ما يسمى تهديدات إرهابية، وعمليات تخريب ونشاطات تجسسية.

٣. هيئة السايبر في الجيش الصهيوني:

لقد اعتبر رئيس هيئة أركان الجيش الصهيوني السابق غابي أشكنازي الفضاء الالكتروني أحد مجالات القتال من الناحيتين الإستراتيجية والعملياتية، وبناءاً على ذلك قام الجيش الصهيوني بتشكيل "هيئة السايبر" في الوحدة ٨٢٠٠ في جهاز الاستخبارات الصهيونية "أمان" بغرض توجيه، وتنسيق نشاطات الجيش الصهيوني في الفضاء الالكتروني.

٤. وحدة إدارة أنظمة المعلومات:

صادقت الحكومة الصهيونية في ٢٧مارس٢٠١١م على إقامة "وحدة إدارة المعلومات، وهي تتبع مدير عام وزارة المالية الصهيونية، ومسئولة مسؤولية مباشرة على جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك مسئوليتها عن مشروع "بنية الحكومة التحتية لعصر الانترنت".

٥. هيئة السايبر الوطنية:

أعلن رئيس الحكومة الصهيونية بنيامين نتنياهو في ١٨مايو ٢٠١١م عن إنشاء هيئة السايبر الوطنية في الكيان الصهيوني، وذكر أن الهدف الأساسي لهذه الهيئة هو تعزيز قدرات الكيان الدفاعية عن أنظمة البنية التحتية الحيوية من هجمات العدو في الفضاء الالكتروني، والتي قد تقوم بها دول أجنبية أو منظمات معادية.

أهم العوامل التي دفعت الكيان الصهيوني الإسراع في اتخاذ الاحتياطات والتدابير الأمنية في الفضاء الالكتروني:

1. **خشية تعرض الفضاء الالكتروني في الكيان الصهيوني إلى حدوث هجمات عليه قد تؤدي إلى إلحاق الشلل بالبنى التحتية الصهيونية، خاصة أنها دولة نووية ومتطورة ومرافقها ومؤسساتها محوسبة.**
2. **تواجه دولة الكيان أعداء لهم دوافع كثيرة لإلحاق الأذى بها كلما استطاعوا تحقيق ذلك، سواء من قبل دول أو منظمات أو أفراد معادين.**
3. **وجود فرص متاحة أمام الكيان الصهيوني لاستعمال الفضاء الالكتروني في الحرب، إلى جانب تطوير دفاعاته المتقدمة.**

تحديات الدفاع في حرب الفضاء الالكتروني:

يعتبر الدفاع في حرب الفضاء الالكتروني تحدياً من نوع جديد للكيان الصهيوني

1. **قدرة العدو على شن هجمات سريعة جداً.**
2. **صعوبة تطبيق سياسة الردع والتي تمثل حجر الزاوية في نظرية الأمن الصهيوني.**
3. **صعوبة تحديد مكان وهوية المهاجم.**

وبالتالي على دولة الكيان إتباع مفهوم "الدفاع الفعال" في الفضاء الالكتروني الذي تتبعه الولايات المتحدة الأمريكية.

ما هو الدفاع الفعال؟

يستند هذا المفهوم على قدرة مخابراتية متطورة لتحديد النشاطات في الانترنت، وعلى أنظمة دفاع ديناميـة ذات رد تلقائي من دون تدخل الإنسان، وهو لا يعتمد فقط على التكنولوجيا المتطورة، وإنما على شبكة محكمة ذات قواعد، وإجراءات صارمة، وعلى ثقافة تفهم المخاطر، وعلى انضباط شديد، وعلى حماية المواقع، وعلى رقابة بشرية قوية.

أهم آراء المحللين والقيادة الصهيونية في استخدام إستراتيجية الحرب الالكترونية في الفضاء الالكتروني:

- **الجنرال يتسحاق بن يسرائيل "رئيس المجلس الوطني للبحث والتطوير":**

أشار إلى وجود فجوة في دولة الكيان بين الاحتياطات الدفاعية عن البنى التحتية الأمنية، وبين الدفاع عن البنى التحتية المدنية الحساسة المهمة ضد هجمات في الفضاء الالكتروني، وأضاف أنها تحدث يوميا، وأنها ليست جزءاً من الخيال، بل هي حقيقة واقعية.

- **عاموس يادلين: "مدير الاستخبارات الصهيونية السابق":**
  - ✓ **إن إسرائيل تطبق التقدم التقني المدني في مجال قدراتها على خوض حرب الكترونية.**
  - ✓ **إن الجيش لديه من الوسائل ما يكفل توفير سبل لأمن الشبكات وشن هجمات الكترونية.**
  - ✓ **إن مجال الحرب الالكترونية يناسب تماما عقيدة الدفاع في إسرائيل.**
  - ✓ **المحافظة على الريادة في هذا المجال مهمة على نحو خاص، في ضوء تغير الإيقاع السريع.**
  - ✓ **إن أحد أهم الأخطار التي تتربص بإسرائيل وقد تلحق بها الأذى تكمن في احتمال اختراق الحواسيب الحيوية الإسرائيلية،**
  - ✓ **إن هيئة السايبر في الجيش تهدف إلى توفير دفاع جيد لشبكات الانترنت العاملة في إسرائيل، وكذلك القيام بهجمات في الفضاء الالكتروني على أهداف خارجية.**

- **يورام كوهين "رئيس جهاز الأمن العام الصهيوني الحالي (الشاباك) ":**

تعتبر الحروب الالكترونية آخر وأحدث أنواع الحروب التي تخوضها إسرائيل ضد أعدائها، لأنها أهم وأخطر أنواع الحروب والتحديات التي تواجه إسرائيل حاليا، بسبب قيام جهات معادية باختراق شبكات الحواسيب بهدف سرقة المعلومات منها أو السيطرة عليها وتعطيل الحياة في كبرى المؤسسات والشركات الحيوية الإسرائيلية.

- **غادي عفرون المدير السابق لحماية المعلومات للبنى التحتية للحكومة الصهيونية:**

طالب بمهاجمة القوى المعادية لإسرائيل باستخدام الحروب الالكترونية، وفقاً لقاعدة "سايبر بدل طائرة، فيروس بدل قنبلة".

- **صموئيل كينان ضابط سابق في هيئة الاتصالات المحوسبة الرئيسي في الجيش الصهيوني:**

إن الهيئة قامت بتحليل التهديدات الالكترونية القائمة، وتوصلت لنتيجة مفادها إن هناك حاجة لتأسيس جهاز لكيفية الحماية والهجوم في مجال السايبر بعد أن باتت ساحة حرب إستراتيجية وفعالة. وأضاف أيضاً إن في حروب السايبر هناك ثلاث مجالات: جمع معلومات،هجوم، ودفاع وهي تعتبر أبعاد مناسبة جداً لمفهوم الأمن في إسرائيل، لأن الجيش يعتزم توفير حماية جيدة للشبكات وتشغيل هجمات الكترونية خاصة به، كما أسسوا في مركز الشيفرة والأمن "طاقم احمر" يعمل بشكل مماثل لسلاح الجو كعدو ودوره اختبار المنظومات الدفاعية.

- حانان غرينبرغ مراسلة عسكرية:

إن عشرات الجنود والضباط الأكاديميين يعملون يوميا، ومعظمهم خريجو البرنامج الرائع "تلفيوت" الذي يعني "الحصن" لتحدي مجال حماية المعلومات في الشبكة العسكرية بشكل هام.

ومما يدلل على عناية الكيان الصهيوني بموضوع الحرب الالكترونية، هو صدور دراسة عن مركز أبحاث الأمن القومي في يونيو ٢٠١١م بعنوان "الحرب الالكترونية ... المفاهيم والتوجهات والأهداف لإسرائيل"، تتناول مفهوم الحرب الالكترونية وأهميتها وتأثيرها بالنسبة للكيان. إضافة لذلك تعتقد الجهات المعنية بهذه المسألة سواء من الجانب العسكري، أو الجانب الأكاديمي أن هذه هي فقط بداية عصر السايبر، لكن التقدير السائد أن الكيان سيوسع قدراته في هذا المجال ولا مانع من أن يعين لهذه المسألة ضابطاً برتبة لواء.

دول العالم التي تسعى إلى تطوير التكنولوجيا الهجومية والدفاعية في مجال الحرب الالكترونية

تنشط العديد من حول العالم في المجال التكنولوجي لتطوير قدراتها في الحرب الالكترونية، وبناء جيوش من الخبراء الذين قد يشكلون نواة الجيش الالكتروني للدولة مثل الصين، روسيا، الولايات المتحدة الأمريكية، فرنسا، انجلترا، إسرائيل وبعض البلدان الأخرى مثل الهند، باكستان، إيران، كوريا الشمالية.

الصين:

- **تعتبر الصين من أكثر الدول التي تعمل على تطوير قدراتها الهجومية في المجال الالكتروني، وهي واحدة من الدول القليلة التي تدمج فعلا مفهوم الثورة في الشؤون العسكرية في صلب عقيدتها العسكرية (التي تعني التجديد ومواكبة التحديات)، وخاصة في مجال الحروب الالكترونية.**
- **تحاول الصين استغلال البعد الالكتروني لتطوير قدراتها اللاتناظرية لتحقيق تفوق في هذا المجال، وضمان قدرات ردعية، وبناء قدراتها التقليدية، واستكشاف نقاط ضعف خصومها في المجال الالكتروني، للتركيز عليها مثل الولايات المتحدة الأمريكية.**

روسيا:

- **تسعى روسيا لتطوير قدراتها في مجال الحرب الالكترونية، خاصة في الشق الهجومي، وهي تعتمد على وسائل أقل تكلفة وأكثر فاعلية في مواجهة الولايات المتحدة الأمريكية وحلف شمال الأطلسي، خاصة منذ إنهيار الاتحاد السوفيتي.**

انجلترا:

- **قامت انجلترا بإصدار إستراتيجية الأمن الالكتروني القومية في يونيو ٢٠٠٩، كما قامت بإنشاء وحدة الأمن الالكتروني، ومركز العمليات ومقره وكالة الاستخبارات القومية، وبدأت عملها في مارس ٢٠١٠م.**

الولايات المتحدة الأمريكية:

- تعتبر الولايات المتحدة من أكثر الدول التي تمتلك القدرات والتقنيات الهجومية العالية المطلوبة في الحروب الالكترونية.
- عمدت الولايات المتحدة على إصدار بعض الخطط والمراجعات في سياسة الفضاء الالكتروني، من أجل تفعيل الأمن الالكتروني ومتطلباته الأولية الأساسية.
- قامت الولايات المتحدة في مايو ٢٠١٠م بإنشاء قيادة الانترنت (سايبركوم) وعينت مدير وكالة الاستخبارات القومية الأمريكية الجنرال كيث أليكساندر للإشراف عليها، وهي تضم ١٠٠٠ فرد من نخبة القراصنة والجواسيس الالكترونيين المحترفين والمميزين.

نماذج من أسلحة الحرب الالكترونية:

ستكنست:

فيروس عبارة عن برنامج كمبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع التي تنتجها شركة سيمنس ايه جي الألمانية. ويقول خبراء أن الفيروس يمكن أن يستخدم في التجسس أو التخريب

- يذكر أن هذا البرنامج قام بمهاجمة أجهزة الحاسوب الموجودة في مفاعل بوشهر الإيراني عام ٢٠١٠م، مما سبب عطلا في أجهزة الطرد المركزي لتخصيب اليورانيوم، وقد أشير بأصابع الاتهام إلى كل من الكيان الصهيوني والولايات المتحدة الأمريكية اللتان تسعيان بشتى الطرق إلى محاربة البرنامج النووي الإيراني.

- لم تكن هذه هي الحادثة الأولى التي تتعرض فيها بعض الدول لمثل هذه الهجمات ففي ديسمبر عام ٢٠٠٩ تعرضت كوريا الجنوبية لهجوم من قبل بعض القراصنة بهدف سرقة خطط دفاعية عن التحركات الكورية والأمريكية خلال الحرب، إضافة إلى ذلك تعرضت ألمانيا في يوليو ٢٠١٠ لعمليات تجسس شديدة ومعقدة من قبل الصين وروسيا استهدفت بعض القطاعات الصناعية والبنى التحتية الحساسة في البلاد.